MODELO BPM PARA LA GESTIÓN DE INCIDENTES INFORMÁTICOS EN LA UNIVERSIDAD LIBRE

JOHN FERNEY CHAVES CELIS
ELBER NÚÑEZ ARAGÓN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

MODELO BPM PARA LA GESTIÓN DE INCIDENTES INFORMÁTICOS EN LA UNIVERSIDAD LIBRE

JOHN FERNEY CHAVES CELIS
ELBER NÚÑEZ ARAGÓN

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Asesor:
JUAN CARLOS ALARCÓN SUESCÚN
Magister en Ingeniería de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, D.C., 12 de septiembre de 2016

DEDICATORIA

A nuestros Seres queridos, Familia y a la Universidad que nos brindó los conocimientos necesarios para que lucháramos y diéramos lo mejor para aplicar lo aprendido en la vida real, finalmente, a todas aquellas personas que de una manera u otra me apoyaron para terminar satisfactoriamente este proyecto.

John Ferney Chaves Celis

Dedico la presente tesis a ti esposa mía, que con tu amor y apoyo siempre me acompañas en el cumplimiento de mis sueños, objetivos y nuevas metas incondicionalmente. A ti hijo que eres la luz de mis ojos, el ser que mueve mi vida. A mis padres, que me enseñaron y forjaron el ser humano que soy ahora y a Dios que por gracia y voluntad me ofrece la oportunidad cada día de tener salud, vida y amor de mis seres más queridos.

Elber Núñez Aragón

AGRADECIMIENTOS

Agradecemos a la Universidad Piloto de Colombia que por su labor de forjar nuevos especialistas y profesionales, nos brindó la posibilidad de ser parte de su *alma mater* en especial al Ingeniero Juan Carlos Alarcón que con su conocimiento, experiencia y tutoría, dimos finalidad a nuestro trabajo de grado y por encima de todo adquirir y apersonarnos de un conocimiento que él nos ofreció.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

GLOSARIO

ATAQUES CIBERNÉTICOS: Symantec se basa en las distintas definiciones de crimen cibernético para describirlo de forma precisa como cualquier delito cometido en el que se haya utilizado un equipo, una red o un dispositivo de hardware. El equipo o el dispositivo pueden ser el agente, el facilitador o la víctima del crimen.[1]

BACKUPS: se define como «copia de seguridad» y permite guardar y almacenar los ficheros, archivos y aplicaciones disponibles en un soporte informático como un teléfono móvil o un ordenador y tiene el objetivo de permitir la recuperación de estos datos a posteriori.[2]

BPM: busca identificar, diseñar, ejecutar, documentar, monitorear, controlar y medir los procesos de negocios que una organización implementa. El enfoque contempla tanto procesos manuales como automatizados y no se orienta a una implementación de software.[3]

CÓDIGO MALICIOSO: software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado. [4]

CONFIABILIDAD: Un sistema es más confiable si es tolerante a errores. La tolerancia a errores es la capacidad de un sistema para seguir funcionando cuando se produce un error en parte del sistema. Para conseguir tolerancia a errores hay que diseñar el sistema con un alto grado de redundancia de hardware.

Si se produce un error en un único componente, el componente redundante asumirá su función sin que se produzca un tiempo de inactividad apreciable.[5]

CONFIDENCIALIDAD: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.[6]

---

[1] NORTON. ¿Qué es un ataque cibernético? [en línea], [consultado el 15 de Junio de 2016]. Disponible en: http://co.norton.com/**cybercrime-definition**/promo

[2] ABC TECNOLOGÍA. ¿Qué es Backups? [en línea], [consultado el 15 de Junio de 2016]. Disponible en: http://www.abc.es/tecnologia/consultorio/20150203/abci-backup-definicion-que-es-201502031524.html

3 IBM. ¿Qué es un BPM? [en línea], [consultado el 17 de Junio de 2016]. Disponible en: https://www.ibm.com/developerworks/ssa/local/websphere/introduccion-bpm/

4 ESET. ¿Qué es un código malicioso? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.eset-la.com/kb/SOLN186

[5] MICROSOFT. ¿Qué es confiabilidad? [en línea], [consultado el 15 de Junio de 2016]. Disponible en: https://technet.microsoft.com/es-es/library/aa996704(v=exchg.65).aspx

CRACKER: la palabra cracker se lleva usando desde los años 80. Se refiere a personas con altos conocimientos de informática que se aprovechan de agujeros de seguridad (bugs, vulnerabilidades, errores de diseño, puntos débiles...) para sacar provecho propio, haciendo actividades que normalmente son ilegales.[7]

CSIRT: significa Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática). El término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, registrado en EE.UU. por el CERT *Coordination Center* (CERT/CC). En general viene a definir a un equipo de personas dedicado a la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio.[8]

DISPONIBILIDAD: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.[9]

FIREWALL: Un firewall actúa a modo de protección de un ordenador local frente a virus, gusanos, troyanos y ataques de hackers.[10]

FreeBSD: es un avanzado sistema operativo para arquitecturas x86 compatibles (incluyendo Pentium® y Athlon™), amd64 compatibles (incluyendo Opteron™, Athlon™64 y EM64T), Alpha/AXP, IA-64, PC-98 y UltraSPARC®. **FreeBSD** es un derivado de BSD, la versión de UNIX® desarrollada en la Universidad de California, Berkeley.[11]

HACKERS: pirata informático. Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta.[12]

---

[6] ARCHIVOS Y GESTIÓN. ¿Qué es confidencialidad? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: archivosygestion.com/garantías/**confidencialidad**

[7] INFORMÁTICA HOY. ¿Qué es un Cracker? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.**informatica**-hoy.com.ar/aprender-**informatica**/Que-es-un-**Cracker**.php

[8] CENTRO DE COORDINACIÓN SEGURIDAD INFORMÁTICA COLOMBIA. ¿Qué es CSIRT? Equipo de respuestas ante emergencias informáticas. [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.**csirt**-ccit.org.co

[9] SGSI. ¿Qué es disponibilidad? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[10] KASPERSKY ¿Qué es firewall? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: http://www.kaspersky.es/internet-security-center/definitions/firewall

[11] FREEBSD ¿Qué es FreeBSD? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: https://www.freebsd.org/es/about.html

[12] DEFINICIONES ABC. ¿Qué significa hacker? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.definicionabc.com/tecnologia/**hacker**-2.php

IDS: es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. [13]

INFORMÁTICA FORENSE: según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.[14]

INTEGRIDAD: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.[15]

NESSUS: Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.[16]

OPERACIÓN: es el conjunto de medios que se ponen en acción para conseguir un resultado previamente determinado mediante una estrategia. Un plan operativo de análisis de riesgos brinda información para el mejoramiento de una estructura[17]

SNIFFER. En informática, un analizador de paquetes es un programa de captura de las tramas de una red de computadoras.[18]

---

[13] MIT. . ¿Qué es un IDS? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

[14] INFORMÁTICA FORENSE COLOMBIA. (s.f.). ¿Qué son los ordenadores cuánticos? ¿Qué aplicaciones tendrán? ¿Es la **informática** del futuro? [en línea], [consultado el 23 de mayo de 2016]. Disponible en:http://www.informaticaforense.com.co/index.php/la-informatica-forense

[15] MICROSOFT. ¿Qué es integridad informática? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: https://msdn.microsoft.com/es-es/library/aa291812(v=vs.7

[16] NESSUS. (s.f.). monitoreo continuo. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: *http://www.tenable.* com/products/nessus-vulnerability-scanner.

[17] CIDBIMENA. ¿Qué es una operación? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: cidbimena.desastres.hn/docum/ops/publicaciones/047/047.7

[18] MUNDOCISCO. ¿Qué es un sniffer? [en línea], [consultado el 23 de mayo de 2016]. Disponible en: http://www.mundocisco.com/2009/08/que-es-un-sniffer.html

INTRODUCCION

La información como parte integral de los activos de una entidad, el intercambio y difusión de la misma dentro y fuera de ella, hacen que la seguridad informática cobre un aspecto relevante para el cumplimiento de los objetivos de negocio propuestos en su razón de ser.

Cuando se integra la seguridad informática a las organizaciones muchas veces se pasa por alto la alineación de los objetivos de negocio con las estrategias, lineamientos, políticas y mejores prácticas, percibiendo un enfoque no claro de los intereses que la organización busca a través de las necesidades del negocio.

La Universidad Libre es una universidad colombiana de carácter privada y con una presencia en seis ciudades del país, por tal motivo la información es un eje que constantemente se encuentra en movimiento y actualización. Es por eso, que la gestión de los incidentes informáticos debe contemplar una estructura que soporte las operaciones del negocio y brindar a la Universidad Libre importantes beneficios como dar respuesta sistemática a los incidentes, prevenir que ocurran reiteradamente, cumplir con la confidencialidad, disponibilidad e integridad de la información, para no afectar el funcionamiento y cumplimiento de los objetivos trazados.

1. PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Universidad Libre tiene varios problemas en cuanto al manejo de la información; debido a que ha ido creciendo progresivamente y no se ha tomado conciencia de la importancia de asegurar la información existente; a medida que avanza es necesario adoptar y crear procedimientos de atención de incidentes de seguridad, que normalicen las buenas prácticas en cada uno de los procesos, transacciones y recursos relacionados con la información y para esto, es preciso efectuar la verificación de riesgos de la seguridad de la información, incluyendo los activos que de forma directa e indirecta están atados a estos procesos.

Si no se integran dentro de la institución, buenas prácticas y recomendaciones de seguridad de la información; es probable que puedan ser víctimas de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

Debido al nivel muy bajo de madurez en los procesos y metodologías internos de la Universidad Libre, es preciso primero establecer un procedimiento de atención de incidentes informáticos con el objetivo de implantar unas bases sólidas que a futuro le sea posible implementar una metodología bpm.

1.2 FORMULACIÓN DEL PROBLEMA

Con el presente trabajo se quiere responder a la pregunta ¿en la actualidad la Universidad Libre en la dirección de sistemas, cuenta con un modelo de procesos, procedimientos, tareas y actores establecido para una adecuada y sistemática atención de los incidentes de seguridad informática?
Incidentes que se puedan presentar de acuerdo con las actividades de la comunidad educativa, comunidad docente y áreas administrativas, que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

1.3 DESCRIPCIÓN DEL PROBLEMA

De acuerdo con la pregunta planteada se realiza la correspondiente investigación evidenciando que la Universidad Libre dentro de sus estrategias de negocio, la seguridad de la información no tiene un mayor protagonismo, debido a que la dirección de sistemas no tiene implantado un procedimiento que permita responder a los incidentes de seguridad de la información de forma sistemática, no cuenta con un plan de concientización sostenible, los recursos con los que cuenta

actualmente no son suficientes, ni con las competencias debidamente adquiridas para soportar la protección de la información e infraestructura.

Estas responsabilidades las delega a terceros que brindan un soporte técnico, pero no se encuentran dentro de un marco de referencia normativo, solo intervienen en la etapa de detección y reporte, pero en las etapas de planificación preparación, seguimiento y cierre y mejora continua, no participan, y no brindan el apoyo suficiente a la Universidad Libre.

También la Universidad Libre hace su aporte con el poco interés de tener actualizada las políticas y de no tener redactado un procedimiento para la atención de incidentes de la información el cual es el objetivo del presente trabajo de grado.

2. JUSTIFICACIÓN

En cada una de las instituciones, empresas u organizaciones, la seguridad de la información ha empezado a tomar un lugar muy importante, con respecto a la manera de gestionar procedimientos de atención de incidentes de seguridad de la información y se ha transformado en un elemento fundamental en la estrategia de negocio con los objetivos de obtener metas significativas al interior de cada organización.

En ese orden de ideas, las empresas advierten la necesidad de definir procedimientos efectivos que avalen una gestión segura de los métodos del *core* del negocio a fin de darle mayor seguridad a la información, y de igual manera evitar tropiezos para adecuarse a los continuos cambios de la organización como resultado de las exigencias del mercado.

La Seguridad de la Información se ha convertido en una necesidad que ha provocado nuevos planteamientos de la administración de tecnologías de la información, fundada en políticas y procedimientos. A su vez, ha orientado el establecimiento de normas, pautas, buenas prácticas, a razón de proteger uno de los activos más valiosos de las empresas como es la información.

Con la llegada de las organizaciones a Internet, se han desplegado un sinnúmero de oportunidades de apertura de nuevos negocios. La protección de la información es un tema que se ha vuelto muy habitual para las organizaciones, ya que es un escenario que comprende desde las actividades más fáciles hasta las situaciones más complicadas relacionadas con el negocio. Así mismo emerge la obligación de consolidar juicios con respecto a la seguridad de la información, por lo que precisamente nace la necesidad de certificar que los contextos de seguridad son óptimos, tanto para las organizaciones como para los usuarios.

El actual proyecto está orientado especialmente, a diseñar y probar un procedimiento para la atención de incidentes de seguridad de la información dirigido a la dirección de sistemas de la Universidad Libre basado en la norma ISO 27035, con el fin de que la dirección de sistemas obtenga una estructura más estándar para atender los incidentes al interior de la Universidad Libre.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar y probar un procedimiento para la atención de incidentes de seguridad de la información dirigidos a la dirección de sistemas de la Universidad Libre, apoyados en la norma ISO 27035, con el propósito de que la Universidad Libre en todas sus áreas pueda mitigar vulnerabilidades de seguridad de la información al interior de la entidad.

3.2 OBJETIVOS ESPECÍFICOS

- Definir las actividades y roles del equipo de atención de incidentes de seguridad.

- Diseñar un plan de concientización de la seguridad de la información para la Universidad Libre.

- Diseñar las actividades para el procedimiento de atención de incidentes de la información para la Universidad Libre.

- Efectuar pruebas sobre el procedimiento de atención de incidentes de seguridad de la Universidad Libre.

4. ALCANCE

Diseñar un procedimiento que le permita a la dirección de sistemas de la Universidad Libre, atender un incidente de seguridad de la información en todas las áreas que pueda presentarse.

Este procedimiento se diseñará apoyado en la norma GTC-ISO/IEC 27035, y constará de las etapas de planificación y preparación, detección y reporte, seguimiento y cierre, mejora continua y pruebas.

Para la etapa de planificación y preparación, se incluye la identificación del equipo actual que integra la dirección de sistemas de la Universidad Libre, se identifican las actividades que se tienen asignadas actualmente y se propone una nueva estructura de organización con la finalidad de mejorar la atención de los incidentes de seguridad de la información. Diseñar un programa de capacitación, que le permita a la dirección de sistemas velar por la disposición de los recursos en la atención de los incidentes.

Para la etapa de detección y reporte, se incluye la identificación y gestión de los elementos que pueden alertar sobre un incidente de seguridad de la información, así mismo la creación de indicadores que nos muestren que ha ocurrido un incidente. La recopilación de información por medio de reportes que el usuario podrá documentar de acuerdo con los indicadores expuestos, que permitirá a la dirección de sistemas de la Universidad Libre responder a los incidentes de forma sistemática.

Para la etapa de seguimiento y cierre, se incluye la creación de una estrategia que permita a la dirección de sistemas tomar decisiones oportunamente para detener la propagación del incidente y evitar que la confidencialidad, integridad y disponibilidad de la información se vea comprometida.

Para la etapa de mejora continua y pruebas, se incluye la creación de los reportes, lecciones aprendidas, medidas disciplinarias, registro en la base de conocimiento. Para la etapa de pruebas, se incluye la creación del plan de pruebas para el procedimiento creado para la atención de incidentes de seguridad de la información en la Universidad Libre, con la finalidad de comprobar si las actividades diseñadas cumplen con los lineamientos de la norma GTC-ISO/IEC 27035 y el problema planteado en la Universidad Libre.

5. DIAGNÓSTICO

En el actual escenario de globalización en el que se encuentra el mundo, en donde las tecnologías de la información han ocupado un papel importante y se han masificado su uso a través de Internet, las organizaciones se ven sumergidas en ambientes de red hostiles donde el vulnerar, perjudicar, hurtar información, se convierten en retos para los ciber delincuentes más conocidos como *Hackers*.

Las tecnologías de la información se han dispersado de forma acelerada por el mundo, asimismo ha crecido el código malicioso y los ataques cibernéticos, los que se han convertido en un constante riesgo, que ha obligado a las compañías y organizaciones a establecer medidas de emergencia y políticas para neutralizar estos ataques maliciosos.

El panorama en Colombia no es ajeno a este flagelo, actualmente muchas instituciones gubernamentales y privadas han sido objeto de ataques de código malicioso, por esta razón el tema de Seguridad de la Información se ha convertido en una necesidad para muchas organizaciones, hasta el punto de incluirla dentro de sus áreas administrativas y en algunas como parte de la mesa directiva.

Realizada la revisión del estado actual de la seguridad de la información en la Universidad Libre, se observó que en la institución no se tienen adelantos en el tema de atención de incidentes de seguridad. Aunque se observa la existencia de normas y procedimientos que cubren distintos aspectos de la Seguridad de la Información, se necesita de forma general de una metodología o un plan de mitigación que soporte a la tipificación de riesgos y determinación de políticas con el fin de contrarrestar los mismos.

Entre los diferentes temas a considerar en la Seguridad de la Información, se identificaron la falta de políticas de seguridad de la información y una categorización de seguridad de los activos de Información de la Universidad. Es de anotar que se identificó la existencia de controles, en el caso de la seguridad lógica, más exactamente acerca de las autenticaciones a los sistemas de información; como también los procedimientos establecidos para el consentimiento de dichas autenticaciones.

Así mismo se evidenciaron controles establecidos con respecto a la seguridad física y de personal. Sin embargo, estos controles no están orientados a una norma de seguridad de la información ni de una evaluación de riesgos a un nivel de una institución educativa. Los controles establecidos a la fecha son producto de evaluaciones particulares realizadas por las áreas involucradas o bajo cuyo ámbito de responsabilidad recae cierto aspecto de la Seguridad.

Posterior al diagnóstico que se realizó en la Universidad Libre, se encontró la falta de un inventario de los equipos y la infraestructura que se hallan en la institución, lo cual hace difícil su administración. Por otra parte, la falta de personal involucrado en la seguridad de la información, hace difícil la concientización, la falta de visión y las limitantes económicas han atrasado el plan de aseguramiento requerido.

Uno de los objetivos principales de la oficina de Sistemas de la Universidad Libre es la de brindar a los usuarios los recursos informáticos con la cantidad y calidad adecuada, con el fin de que se tenga la continuidad del negocio y la disponibilidad del servicio. De este modo la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el Centro son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe de plasmar mecanismos confiables que con base en la política institucional proteja los activos del centro educativo.

En conclusión, ante este panorama surge el siguiente proyecto de políticas rectoras que harán que la Oficina de Sistemas pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere en particular a la gestión de incidentes de seguridad de la información.

6. MARCO TEÓRICO

6.1 DEFINICIONES BÁSICAS

Cuando hacemos referencia al término diseñar un procedimiento, nos referimos al conjunto de acciones u operaciones que tiene que realizarse de la misma forma para obtener un mismo resultado sobre las mismas circunstancias. Cuando hacemos referencia a un incidente de seguridad de la información es todo evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Al combinar las anteriores definiciones, se quiere diseñar un procedimiento que le permita a la Universidad Libre, atender un incidente de seguridad de la información, y para que este procedimiento pueda ser ejecutado de la misma forma en diferentes circunstancias se toma como apoyo la siguiente norma con la finalidad de seguir una pauta internacional:

6.1.1 NTC-ISO-IEC 27035 - Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. La norma brinda orientación sobre la gestión de incidentes de seguridad de la información para empresas grandes y medianas. Las organizaciones más pequeñas pueden usar un conjunto básico de documentos, procesos y rutinas descritos en la presente guía, de acuerdo con su tamaño y tipo de negocio, en relación con la situación de riesgo de seguridad de la información. También brinda orientación para organizaciones externas que prestan servicios de gestión de incidentes de seguridad de la información**.**[19]

6.2 ETAPAS DE ATENCIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Dentro del procedimiento que se propone para la atención de incidentes de seguridad de la información para la dirección de sistemas de la Universidad Libre, son necesarias abordar las siguientes etapas que comprenden su ciclo de vida:

[19] MINISTERIO DE LA TECNOLOGÍA, INDUSTRIA Y COMERCIO. Normas NTC-ISO-IEC 27035 - Tecnología de la información. [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_Continuidad.pdf

6.2.1 Planificación y preparación. La etapa de preparación incluye todas aquellas actividades que le permitan a la dirección de sistemas de la Universidad Libre de forma proactiva, tener las herramientas necesarias para responder y hacerle frente a un incidente de seguridad informática, garantizando que los recursos, infraestructura y miembros estén definidos y apoyados por las directivas de la entidad, en esta etapa se integran actividades de sensibilización, definición de procedimientos, actividades de entrenamiento, ensayos y evaluaciones de seguridad, análisis de alertas y amenazas, análisis de mejora continua de procesos y el planteamiento de un esquema de roles y funciones que llevaran a cabo la ejecución de las diferentes etapas.

6.2.2 Detección y reporte. En esta etapa se realizan actividades encaminadas a la detección e identificación de las diferentes anomalías que pueden estar presentes dentro de la infraestructura, aplicaciones, red y su comportamiento en general, en esta etapa las actividades incluidas son: recepción de reportes de incidentes, categorización de incidente, valoración de impactos, elaboración del plan de respuesta al incidente, elaboración de medidas de contención y mitigación, elaboración de informes.

6.2.3 Seguimiento y cierre. Esta etapa comprende la elaboración del análisis pos incidente el cual se deberá llevar una investigación que determine la magnitud del incidente y los mecanismos de prevención del impacto, revisar las políticas con la finalidad de realizar los ajustes si aplican y documentar los hechos para alimentar la base de conocimiento.

6.2.4 Mejora continua. En esta etapa se revisará la documentación generada y se llevaran a cabo las reuniones con el equipo conformado por la dirección de sistemas de la Universidad Libre para realizar las diferentes retroalimentaciones que complementen la base de conocimiento y se afinen destrezas y se refuerce el conocimiento en la atención de los incidentes de seguridad de la información.

6.3 CONTEXTO DE LA SEGURIDAD EN LA UNIVERSIDAD LIBRE

Se muestra a continuación los procedimientos y políticas de seguridad de la información, instauradas por la Universidad Libre; que se encuentran orientadas a la Confidencialidad, Integridad y Disponibilidad de la información.[20]

[17] UNIVERSIDAD LIBRE DE COLOMBIA. Seguridad de la información. [en línea], [consultado el 23 de mayo de 2016]. Disponible en: https://www.unilibre.gov.co/.../**Por**tals/0/**Documentos**/

6.3.1 Normas de seguridad en la Universidad Libre. Normas relacionadas con el ingreso de funcionarios, la confidencialidad de la información y la aceptación de las políticas de seguridad.

6.3.1.1 Normas Dirigidas a: TODOS LOS USUARIOS. Está orientada a todos los usuarios de la Universidad, la cual indica que se debe firmar un acuerdo de confidencialidad y otro de cumplimiento de políticas de seguridad de la información; esta labor debe realizarse antes de que la persona se vincule a la Universidad como empleado y se le suministren credenciales de acceso a los sistemas de información.

6.3.2 Política Global de Seguridad de la Información. Para la universidad la información es un activo preciado y también tiene un valor crítico orientados a cumplir los objetivos de la razón de ser de la entidad, la información es la base para definir las decisiones que preserven las ventajas competitivas de la institución.

Todos los usuarios que tienen funciones sobre los repositorios y recursos de los sistemas de información de la corporación, deben ajustarse a las políticas del acuerdo de seguridad de la información, lo anterior para mantengan una discreción y confidencialidad, con el fin de garantizar la integridad y disponibilidad de la información, de igual forma minimizar las vulnerabilidades de la misma.

A su vez la Jefatura en conjunto con la Auditoría interna de la Universidad, con el fin de velar por la aplicación de los controles en los procedimientos de la institución, con la finalidad de garantizar los tres pilares de la información: Confidencialidad, Integridad y Disponibilidad.

6.3.2.1 Políticas de uso de las comunicaciones electrónicas (correo electrónico). La razón de ser del correo electrónico se debe a que suministra la comunicación entre toda la comunidad administrativa y estudiantil, asimismo como proveedores y terceros. Es necesario avalar que su uso sea para fines institucionales; siguiendo los lineamientos de la confidencialidad, integridad y disponibilidad.

6.3.2.2 Políticas de asignación de responsabilidades operativas. La Jefatura de Sistemas, es el ente al interior de la Universidad que se encarga de la gestión de la plataforma de infraestructura y tecnológica, con el fin de apoyar los procesos del negocio, de igual forma delega ocupaciones a los funcionarios, quienes a su vez deben velar por los procedimientos orientados a las buenas prácticas gestión de dicha plataforma.

6.3.2.3 Políticas de intercambio de información. Es necesario que cualquier tipo de intercambio de información sensible, entre las seccionales o unidades administrativas o académicas de la Universidad o de igual forma con externos; deba efectuarse siguiendo las políticas del Acuerdo de Seguridad de la Información.

6.3.2.4 Políticas de administración y protección de la Información. Los usuarios de la Universidad Libre y el personal externo como: proveedores, etc. Se encuentran en la obligación de ser garantes en la integridad, disponibilidad de la información que manipulan y suministran. También como el buen manejo de los recursos tecnológicos de la institución. [21][18]

6.4 IDENTIFICACIÓN DE ROLES

Actualmente en la dirección de sistemas de la Universidad Libre se encuentra publicado el organigrama que se presenta en la Figura 1.Organigrama dirección de sistemas Universidad Libre, este organigrama en la realidad no corresponde a los roles que se encuentran actualmente ejecutando las área de operaciones de la Institución.

Dentro de la investigación se encontró los siguientes recursos los cuales soportan el área de operaciones:

Jefe de Sistemas. Es la persona encargada de proyectar, estructurar y conservar los sistemas, métodos y procesos de información. También de administrar la política de tecnologías de la comunicación para que se alinee los objetivos y lineamientos de la Universidad, de igual forma indica el plan informático de acuerdo con los objetivos a corto, mediano y largo plazo. Por otro lado, establece las soluciones informáticas para resguardar las necesidades de los usuarios y de la Universidad.

[21] UNIVERSIDAD LIBRE DE COLOMBIA. Políticas de seguridad de la administración y protección de la Información en la Universidad Libre. . [en línea], [consultado el 23 de mayo de 2016]. Disponible en: www.uni**libre**.edu.co/...**univ**ersitarias/153-nuestro-sistema-de-gestion-de-**seguridad**

Coordinador de Sistemas. Dentro de las funciones de esta persona se encuentra el de regularizar el soporte técnico preventivo y correctivo de hardware, software y comunicaciones del modo que se avale su considerada operación y funcionamiento. Así mismo está el de atender las solicitudes de información necesarias para la ejecución de las pruebas de sistemas de información obtenidos a los proveedores, a través de la realización y la gestión de los proyectos que estos soliciten.

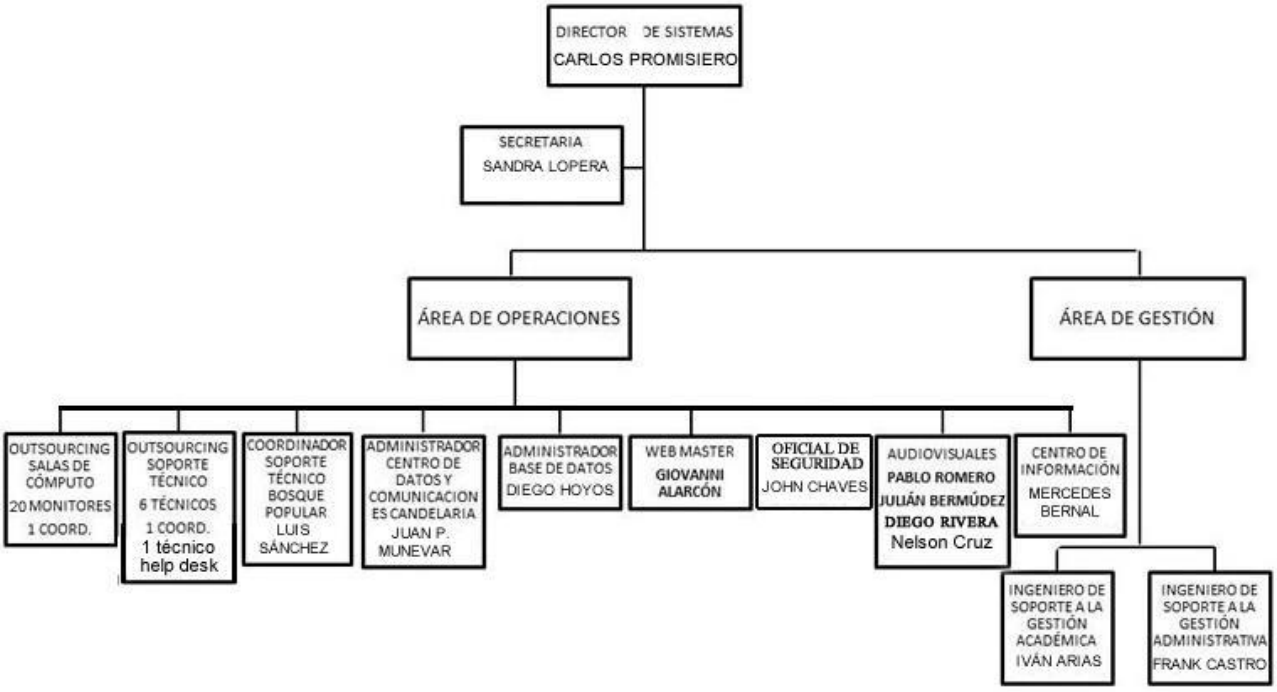
Administrador de Bases de Datos. Él es el encargado de responder por las solicitudes de información necesarias para la ejecución de las pruebas de aplicaciones y de igual forma a los sistemas de información obtenidos a proveedores a través de la producción de los programas que estos soliciten. Ejecutar la actualización de las aplicaciones adquiridas a terceros, conforme con los parámetros de datos e información definidos previamente y a los cambios solicitados por las otras dependencias.

Oficial de Seguridad. Es la persona que debe estar preparada para plantear, efectuar y conservar destrezas y componentes de seguridad que salvaguarden la disponibilidad y uso de los recursos informáticos. Gestionar la infraestructura de Red de Datos, cableada e inalámbrica, y de igual forma la de seguridad como Directorio Activo, *Firewall*, Antivirus, etc.

Web Master. Gestionar y ejecutar el mantenimiento del portal web de la Universidad, custodiar por la integración de las páginas web de las seccionales y regularizar los proyectos de actualización. Evidenciar toda la operación del portal y los métodos requeridos para su reajuste.

A continuación en la figura 1 se describe el organigrama de la Universidad Libre

Figura 1. Organigrama dirección de sistemas Universidad Libre



Fuente: autores

7. DISEÑO DEL PROCEDIMIENTO

7.1 PROCEDIMIENTO DE PLANIFICACIÓN Y PREPARACIÓN

Dentro de la planificación y preparación se iniciará con el planteamiento del siguiente esquema de roles y las funciones que se deberían implantar al interior de la dirección de sistemas de la Universidad Libre:

7.1.1 Jefe de Sistemas. Aparte de las funciones designadas para el Jefe de Sistemas, también es necesario que se generen funciones y actividades relacionadas con la atención de incidentes de seguridad.

La razón de responder adecuadamente a los incidentes de seguridad tiene sus beneficios indudables. Sin embargo, también pueden existir beneficios indirectos. En el caso de las notas de los estudiantes, si se puede demostrar que la Universidad está en la capacidad de contrarrestar y manejar los ataques de manera ágil y eficaz, esto genera confianza por parte de los usuarios que en este caso serían los estudiantes de la institución y acrecentaría el prestigio y la credibilidad de la misma, ya que esto muestra que la entidad está alineada con las políticas de seguridad de la información. A continuación, estos son los ítems que el Jefe de Sistemas debe tener en cuenta para atender manera apropiada un incidente:

- Establecer un grupo CSIRT (*Computer Security Incident Response Team*, por sus siglas en Ingles)
- Concretar un procedimiento de respuesta a incidentes.
- Disminuir la cuantía y gravedad de los incidentes de seguridad.
- Contener los daños y minimizar los riesgos.

Ante la ausencia de un grupo que atienda los incidentes de seguridad, se hace necesario que el jefe de Sistemas establezca un grupo CSIRT para el trato de los incidentes de seguridad de la Universidad. Aunque la creación de un grupo como tal demanda una labor compleja y extensa en cuanto preparación de las personas, tecnología, infraestructura y presupuesto, la dirección de sistemas podrá iniciar con un equipo conformado por un grupo de personas idóneas para atender los incidentes de seguridad con la finalidad de sentar las bases que a futuro y en un estado de madurez avanzado puedan conformar el CSIRT que la Universidad Libre establece en sus lineamientos. Los integrantes del equipo deben haber determinado claramente sus labores para afirmar que no quede ninguna dependencia o área de la respuesta sin cobijar.

Se debe tener en cuenta que el equipo que se conforme, debe realizar las siguientes funciones:

- Evidenciar y relacionar los incidentes de seguridad.

- Deben incrementar el nivel de conciencia en proporción a la seguridad al interior de la entidad con el fin de ayudar de impedir que se ocasionen incidentes en la Universidad.

- Facilitar las auditorías de sistemas, con el fin de evaluar los procesos como y obtener las vulnerabilidades y pruebas de *pentesting*.

- Deben recolectar información acerca de las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.

- Supervisar los sistemas en busca de infracciones de seguridad.

- Investigar acerca de nuevas revisiones de software.

- Investigar y desplegar nuevas tecnologías para disminuir los riesgos y de seguridad.

- **Recolectar evidencias digitales.** Para casos de informática forense en que el jefe de sistemas tenga que realizar el direccionamiento, este deberá seguir los procedimientos establecidos a la cadena de custodia, la cual debe ser clara y suficiente. El análisis debe ser solo sobre copias del material de la evidencia, se debe registrar cuando y donde fue ejecutado el proceso de copiado, quien realizo las actividades y que herramientas y programas fueron utilizados.

Se proponen las anteriores funciones para la Universidad Libre como punto de inicio para un equipo de incidentes que apenas iniciaría las labores, con miras a sentar unas bases de conocimiento y práctica, que con el tiempo se irán incrementando las actividades y el campo de acción; cada vez que su experiencia y madurez avance y se puedan establecer otros lineamientos más profundos

7.1.2 Coordinador de Sistemas. Junto con el Oficial de Seguridad, son las personas que se deben preparar el equipo CSIRT para tratar los incidentes de seguridad. Para conformar el equipo, es necesario instruirlos acerca del uso apropiado y la utilización de las herramientas de seguridad informática. De igual forma es necesario suministrarles equipos de cómputo con estas herramientas, de forma que puedan atender a los incidentes informáticos. Estos sistemas y las herramientas asociadas deben estar protegidos adecuadamente.

El Coordinador de Sistemas es el encargado de administrar el área de soporte de TI, por ende, debe instituir visiblemente y poner en práctica todas las políticas y procedimientos al interior de la Universidad. Diversos incidentes de seguridad están ocasionados de manera accidental por el personal de TI, que en algunos casos no han seguido o no han entendido las políticas de administración de cambios, o bien no han configurado adecuadamente los dispositivos de seguridad, en el caso de firewall o los sistemas de autenticación. De acuerdo a lo anterior, es necesario que el coordinador establezca procedimientos y que a su vez se les pueda realizar pruebas exhaustivas a estos, con el fin de garantizar que son prácticas y claras, asimismo que ofrezcan el nivel de seguridad requerido.

7.1.3 Oficial de Seguridad. El Oficial de Seguridad debe preparar al equipo CSIRT. Para ésta preparación del equipo, se deben seguir los siguientes ítems:

Es necesario reunir la información de comunicación pertinente. Debe confirmarse que cuenta con los nombres y números de teléfono de contacto de las personas de la Universidad a las que sea necesario avisar (incluso los integrantes del CSIRT). Asimismo, se requiere información del proveedor de servicios de Internet (ISP) y las autoridades locales y nacionales (CERT, Centro Cibernético Policial entre otros). También se debe contar con la asesoría legal para contactar a las autoridades locales pertinentes antes de que se materialice un incidente. De ésta forma se contribuirá a afirmarse que se comprenden las operaciones convenientes para informar los incidentes y la constitución de pruebas. En el caso de cualquier eventualidad es necesario avisar a la asesoría legal de la autoridad que concierne.

Ilustrar al grupo en la manipulación adecuada de las herramientas de seguridad críticas. De igual forma suministrarles equipos portátiles configurados con estas herramientas para certificar que no se malgasta tiempo en la instalación y configuración de las herramientas, de modo que puedan responder a los incidentes. Estos sistemas y las herramientas asociadas deben estar protegidos adecuadamente cuando no se usen.

Se debe publicar la información del sistema de emergencia en un sitio central y que no posea conexión de ninguna clase, se debe transmitir en una carpeta física o un equipo de cómputo que no tenga conexión. Esta información de emergencia incluye las contraseñas de los sistemas, las direcciones IP, la información sobre la configuración de los enrutadores, las listas de conjuntos de reglas del firewall, copias de las claves de entidad emisora de certificados, los nombres y números de teléfono de contacto, los procedimientos de extensión, etc. Esta información debe estar disponible con facilidad y se debe mantener en un lugar seguro. Un método para proteger y hacer esta información fácilmente disponible consiste en cifrarla en un equipo portátil de seguridad dedicado, guardado en una caja fuerte con acceso limitado a ciertos individuos, como el coordinador del CSIRT, o el director del departamento informático o tecnológico.

Una vez definidos los roles y sus funciones, se deberá continuar con una serie de actividades enmarcadas en una planificación y preparación que permitan el

seguimiento y soporte transversal a los procesos que se realizan dentro de la Universidad Libre, con la finalidad de garantizar la información en cada momento e integrar los diferentes actores al procedimiento de seguridad de la información.

7.2 ACTIVIDADES DE SENSIBILIZACIÓN

Se debe desarrollar planes relacionados con cultura en seguridad de la información, teniendo en cuenta elementos como: concientización, entrenamiento y educación. De acuerdo con lo anterior, estos elementos hacen que las actividades relacionadas con la cultura de seguridad de la información se interioricen y se ponga en práctica por parte del usuario final y las directivas. Los contenidos están dirigidos a dos grupos: directivos, personal administrativo y/o comunidad estudiantil.
A continuación, los temarios deben contener la siguiente información que se van a tratar en las charlas de sensibilización:

Charla sensibilización para el Grupo Directivo y Jefes de Unidades. Conocer los conceptos sobre seguridad de la información.

- ¿Por qué es importante la Seguridad de la Información?
- ¿Qué debo proteger?
- ¿De quién me debo proteger?
- Eventos de Seguridad
- Por qué son importantes las Políticas de Seguridad
- Ronda de Preguntas

Charla Sensibilización para la Comunidad / Usuario final. Conocer los conceptos sobre seguridad de la información como denunciar y la legislación existente.

- ¿Por qué es importante la Seguridad de la Información?
- ¿De quién me debo proteger?
- ¿Eventos de Seguridad?
- ¿Cómo debo actuar?
- ¿Legislación Colombiana?
- ¿Recordatorios?

7.3 DEFINICIÓN DE PROCEDIMIENTOS

7.3.1 Procedimiento de ingreso al centro de cómputo y centros de cableado. Se hace necesario definir un procedimiento que tenga como objetivo establecer el ingreso al centro de cómputo y centros de red para que sea uniforme tanto para funcionarios de la Universidad como para los contratistas.

De igual forma, se debe describir los mecanismos de control de acceso para visitantes que soliciten acceso a las áreas de TI y a los centros de red de la Universidad Libre, esto es importante y necesario, por tratarse lugares donde reside información sensible.

7.3.2 Procedimiento de aseguramiento de servidores. El objetivo es detectar y corregir los problemas de seguridad sobre la institución, que puedan poner en riesgo la seguridad de los mismos y por ende la seguridad de la información.

Se debe puntualizar los cambios a efectuar en los diferentes elementos de la institución con el fin de atenuar los problemas de seguridad. Estos cambios se deben representar en una matriz de riesgos, donde se detallan los problemas hallados, los riesgos que se muestran, el modo de solucionarlo y las observaciones pertinentes.

Indicar en su totalidad las correcciones a efectuar, de igual forma se debe validar previamente con los administradores de cada uno de los servidores de la Universidad, a fin de evaluar los alcances de los cambios propuestos.

Es necesario definir los cambios requeridos que se van a realizar en la institución con el fin de optimizar el nivel de seguridad. Los cambios anteriormente requeridos, se deben representar en la matriz mencionada anteriormente que contempla aspectos como:

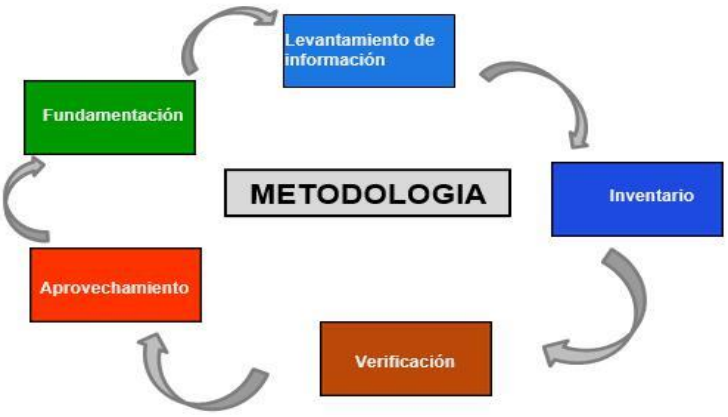
- Actualización de seguridad en los servidores.
- Verificación de permisos de archivos y carpetas.
- Comprobación de permisos de usuarios.
- Servicios innecesarios
- Aplicaciones innecesarias
- Archivos de inicio
- Mecanismos de auditoria
- Mecanismos de administración
- Restricciones de acceso a los usuarios
- Auditorias de contraseñas
- Interacción con software de gestión.

- Interacción con otros tipos aplicaciones de seguridad (*Firewalls, IDS, backups,* etc.)

7.3.3 Procedimiento de implementación de backups en estaciones de trabajo. Tiene como finalidad realizar el almacenamiento de forma segura de toda la información digital que dentro del desarrollo de las funciones se considere documental, importante y crítica, generada en cada una de las unidades académicas y administrativas de la Universidad Libre.

7.3.4 Metodología de ethical hacking. Se hace necesario establecer una metodología de *Ethical Hacking*, la cual se debe desarrollar de acuerdo con lo definido por las metodologías OSSTMM y OWASP (Metodología orientada a pruebas de intrusión a aplicaciones) manifestada en el siguiente diagrama que describe las etapas para el levantamiento de información, inventario, verificación, aprovechamiento y fundamentación. En la Figura 2 Metodología *Ethical Hacking* se ilustran las etapas.

Figura 2. Metodología Ethical Hacking



Fuente: autores

7.3.4.1 Levantamiento de información. Se debe realizar un levantamiento de la información al interior de la Universidad con el fin de encontrar objetivos como: servidores, enrutadores, firewalls y demás accesos en las redes. Conforme al escenario seleccionado para realizar las pruebas, se pueden encontrar las siguientes situaciones:

- Pruebas Ciegas, son denominadas pruebas de caja negra de acuerdo a la metodología OSSTMM, porque no se suministra ningún tipo de información y se

lleva a cabo la tarea de descubrimiento de la misma, para la planeación del ataque. En este tipo de escenarios las pruebas toman más tiempo por cuanto se debe recolectar más información inicialmente, a través de herramientas de búsqueda como Google, Bing, etc.

- Pruebas con Información, se definen de esta forma porque los administradores de infraestructura facilitan información básica de sus redes, servidores, etc. y de esta forma se puede mejorar el tiempo de las pruebas orientándolas a los objetivos más específicos.
- Pruebas con cuenta creada y validación a nivel de un usuario nivel medio.

- Pruebas sin protección de los dispositivos de protección perimetrales (Resguardando todas las medidas para proteger los sitios a explorar).

7.3.4.2 Inventario. Se debe realizar un proceso de inventario, en el cual se consiguen y cataloga información importante, de acuerdo con lo anterior se precisan los posibles vectores de ataque. Como parte de esa información esta:

- Enrutamiento
- Nombres de usuarios
- Servicios y aplicaciones
- Puertos abiertos
- Conexiones externas

7.3.4.3 Verificación. Radica en establecer problemas de seguridad, de acuerdo con los resultados del inventario y el levantamiento de información, y los potenciales vectores de ataque. Estos problemas de seguridad de la información se pueden hallar utilizando software especializado o de manera manual. La verificación de las vulnerabilidades encontradas puede demorar más tiempo, ya que, para tener mayores posibilidades de éxito, se requiere establecer los falsos positivos. Como resultado de la verificación de vulnerabilidades, se estipula la estrategia a seguir durante las pruebas de intrusión.

7.3.4.4 Aprovechamiento. Atacar los objetivos escogidos en la fase anterior aprovechando las vulnerabilidades descubiertas. Dentro de la etapa del ataque, se prueba la existencia real de las vulnerabilidades encontraras en las etapas anteriores, para así determinar el impacto de las mismas. Al interior del desarrollo de la etapa de aprovechamiento, pueden surgir nuevas vulnerabilidades no detectadas en las etapas anteriores, las cuales serán incluidas dentro de esta fase, para su verificación.

7.3.4.5. Fundamentación. Elaboración de un informe pormenorizado con los resultados logrados durante todo el proceso de ejecución de las pruebas de penetración, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura informática de la Entidad. Con las recomendaciones requeridas para solventar los problemas mencionados que se encuentran alineados según normas internacionales como la norma ISO 27002 -27001.

7.4 PROCEDIMIENTO DETECCIÓN Y REPORTE

La detección de incidentes se puede generar de forma automática por medio de sistemas de seguridad implantados dentro de la Universidad Libre, caída de servidores, sistemas de antivirus o de forma manual por medio de reportes realizados por funcionarios, monitoreo, revisión de logs, información expuesta a funcionarios no autorizados. Al momento de ocurrir una detección de incidente es necesario seguir con las siguientes actividades:

7.4.1 Advertir de la posibilidad de un incidente de seguridad de la información. Ante un posible incidente de seguridad se advertirá a la Mesa de Ayuda a través de los siguientes canales:

• Debe enviar un mensaje a través de correo electrónico a soporteti@unilibre.edu.co.

• A través de llamada telefónica a la Mesa de Ayuda a la extensión 1138.

El funcionario que informe sobre el posible incidente de seguridad, debe tener en cuenta los siguientes lineamientos en el momento de generar el reporte:

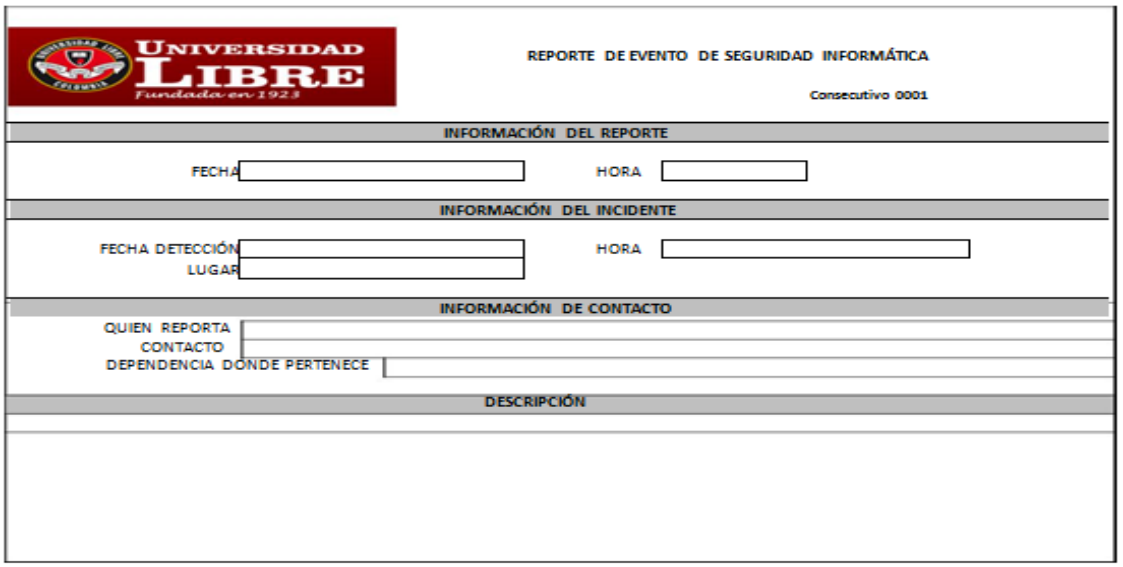
• Constituir por qué se piensa que se está tratando de un incidente de seguridad que afecta la confidencialidad, integridad y disponibilidad.

• Integrar toda la información que llevó a establecer que es un incidente, información que podrá ser empleada en la investigación y/o para iniciar a mitigar los daños y menguar el riesgo.

Esta consolidación de la información se empleará a futuro para documentar el incidente (ya sea real o falso). La consolidación de la información se realizará por medio de la estructura descrita en la figura 3 Reporte Evento seguridad, que contiene una información del reporte: fecha y hora, información del incidente: fecha de detección, lugar y hora, información del contacto: quien reporta el incidente, información de contacto y la dependencia a donde pertenece, por último, se relaciona una sección de descripción donde se relacione que es lo sucedido.

En la figura 3 se describe el reporte de evento de seguridad.

Figura 3. Reporte Evento seguridad



Fuente: autores

7.4.2 Documentación del incidente de seguridad de la información. En el momento que se realice la recepción de la notificación de un incidente de seguridad, la Mesa de Ayuda debe realizar la primera clasificación del Incidente, en la Herramienta de Mesa de Ayuda para empezar con la atención del mismo, allí se creara un *Ticket*.

De igual forma se emplean definiciones como Incidente y Solicitud Inicial respectivamente, los cuales pueden ser asociados a los tickets según corresponda, a continuación; se muestra las siguientes definiciones:

- Solicitud Inicial: Se emplea cuando se genera un reporte de evento de seguridad porque puede generar varios tickets para su tratamiento, siendo la solicitud inicial la que afianza la información del incidente.

- Incidente Inicial: Se emplea cuando el reporte de evento de seguridad es confirmado y es posible que sea compuesto por varios tickets que traten una misma situación.

En el incidente inicial es necesario profundizar la información contemplada en la solicitud inicial, esta información deberá ser consignada en la estructura de reporte

de incidente informático descrita en la Figura 4 Reporte Incidente Informático, en este reporte se describe la fecha del incidente, el número de incidente, la información del contacto, la información del incidente, esta información es diligenciada de acuerdo a la categorización de incidentes de seguridad que se establezca, una descripción de lo sucedido y que componentes fueron afectados.

Figura 4. Reporte Incidente Informático

Fuente: autores

La información allí recopilada deberá ser almacena con la finalidad de alimentar la base de datos de incidentes presentados.

7.4.3 Categorización de incidentes de seguridad de la información. Para una apropiada administración, todos los incidentes deberán estar categorizados. Un incidente que contenga múltiples clases o tipologías debe ser clasificado por el evento de seguridad original.

A continuación, en el cuadro 1 categorización de Incidentes se analiza la categorización de incidentes para la Universidad Libre que contiene una categorización de incidentes que se pueden presentar, la clase a que corresponde y una definición del mismo.

Cuadro 1. Categorización de Incidentes

Categorización	Clase	Definición
Ataques	Explotación de *Backdoor*o puertas traseras	Perjuicios, ausencias o puestas en riesgo de la información de la Universidad Libre por explotación de *Backdoor*o o puertas traseras dejadas en los procesos de diseño de aplicaciones y sistemas de información
	Explotación de debilidades informáticas	Perjuicios ausencia opuestas en riesgo de la información de la Universidad Libre por aprovechamiento de vulnerabilidades de los sistemas de información.
	Denegación de servicios	Perjuicios, ausencia o puesta en riesgo de la información de la Universidad Libre cuando se presentan eventos que ocasionan perdida de un servicio tecnológico en particular. Los síntomas para detectar un incidente de esta categoría son: Tiempos de respuesta muy bajos sin razones aparentes, servicios internos inaccesibles sin razones aparentes, servicio(s) externo(s) inaccesibles sin razones aparentes.
	Escaneo de redes	Perjuicios ausencia opuesta en riesgo de la información de la Universidad Libre, por intentos de adivinar, quebrantar y/o violentar contraseñas.
	Intentos de acceso	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por intentos de adivinar, quebrantar y/o violentar contraseñas.
Daños físicos	Interferencia	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por interferencias que obstruye las redes de computador, de radio y/o televisión por cableado o inalámbrico a través de medios técnicos.

Continuación cuadro 1.		
Categorización	Clase	Definición
Daños físicos	Agua	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a agua dentro de las instalaciones de la Universidad Libre.
	Ambiente infortunado	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a contaminación, polvo, moho.
	Destrucción de equipos	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre por causas asociadas a destrucción de equipos o medios con información
	Incendio	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a incendios dentro de las instalaciones de la Universidad Libre.
Desastre natural	Inundaciones naturales	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a inundaciones generadas por ríos, quebradas, etc.
	Terremotos	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a terremotos
	Granizo	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a granizo
Daño a infraestructura tecnológica	Daño físico	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a daños físicos.

Continuación cuadro 1.		
Categorización	Clase	Definición
Daños físicos	Error de funcionamiento del software	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a error de funcionamiento de un software.
	Quebrantamiento de mantenimiento	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a error en los mantenimientos establecidos por la Universidad Libre.
Daños a infraestructura física	Daño alimentación eléctrica	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a daño en la alimentación eléctrica
	Daño en aire acondicionado	Perjuicios, ausencia opuesta en riesgo de la información de la Universidad Libre, por causas asociadas a inconvenientes en los aires acondicionados.
Malware	Botnet	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por causas asociadas a Botnet.
	Gusano de red	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por causas asociadas a programa(s) malicioso(s) diseminado(s) y replicado(s) en la red de la Universidad Libre.
	Página Web con código malicioso	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por causas asociadas a páginas web con código malicioso.
	Sitio hosting con código malicioso	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por sitio de alojamiento de un código malicioso descargado por usuarios objetivo.

Continuación cuadro 1.		
Categorización	Clase	Definición
Malware	Troyanos	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por causas asociadas a troyanos
	Virus informático	Perjuicio, ausencia o puesta en riesgo de la información de la Universidad Libre, por causas asociadas a virus informáticos
	Interceptación	Interceptar una conversación de una parte externa sin que esta tenga conocimiento.
	Divulgación	Dar a conocer públicamente información confidencial o reservada.
Puesta en riesgo de la información	Fisgoneo	Recaudación secreta de información y la divulgación de esta acerca de los procesos de la otra institución.
Puesta en riesgo de la información	Ingeniería social	Recolección de información de una persona utilizando medios no técnicos
	Interceptación	Captura de datos antes de que puedan llegar a los usuarios previstos
	Phishing	Perjuicios, ausencia o puesta en riesgo de la información de la Universidad Libre por Phishing.
	Robo de información	Apropiación de datos sin previa autorización.
Fuente: autores		

7.5 VALORACIÓN DE CRITICIDAD DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para una adecuada administración, todos los Incidentes de seguridad deberán estar clasificados según su estado crítico y la afectación a la Universidad Libre, el cuadro 2 valoraciones criticidad de Incidentes, muestra una valoración de criticidad de acuerdo al inventario de activos de la Información de la Universidad Libre.

Cuadro 2. Valoraciones criticidad de Incidentes

Valoración	Descripción
CRITICA	Es un suceso que simboliza una seria amenaza para la Universidad Libre, que altera de forma inmediata a uno o más recursos importantes, pone en peligro información confidencial de la Universidad Libre se considera de gran afectación para la misión de la institución y/o sistemas de misión crítica. En esta valoración cada uno de estos incidentes puede originar la pérdida total de sistemas de misión crítica, que están directamente relacionados con la continuidad del negocio de la Universidad Libre, inclusive podrían afectar la seguridad física de las personas, causar una pérdida irreversible de recursos de la entidad y/o resultar en cargos criminales.
ALTA	Se categorizan en este nivel de criticidad los incidentes de los cuales se tiene constancia que son una amenaza que ha afectado o esta afectando los activos categorizados como muy altos en confidencialidad, integridad y/o disponibilidad para la Universidad Libre. El incidente catalogado de alta criticidad tiene un impacto desmedido (afectación total a la confidencialidad, disponibilidad o integridad) en la información y se considera crítica para la misión de la Universidad Libre, esto incluye información en diferentes medios y/o sistemas críticos. Estos incidentes suelen causar la degradación de los servicios vitales para un gran número de usuarios, implican una grave violación de seguridad, afectan a los equipos vitales o servicios, o pueden dañar la confianza en la administración pública o podrían afectar la seguridad física de las personas, causar una pérdida importante de recursos de la Universidad Libre.
BAJA	Se categorizan con este nivel aquellos eventos que puedan ser una amenaza que afecta o está afectando a activos de una amenaza que afecta o esta afectando a activos de información de la Universidad Libre con una valoración de impacto limitado en tres pilares de la información (confidencialidad, disponibilidad o integridad. La Universidad libre debe contar con controles de seguridad desplegados, funcionales que contrarrestan adecuadamente estos eventos, por lo tanto, su impacto debe ser nulo o mínimo. La Universidad Libre ya debe estar capacitada para gestionar estos incidentes y tener desplegados controles que elimine o limiten sus riesgos.
Fuente: autores	

Para establecer el nivel de criticidad debemos tener en cuenta un impacto alto, medio o bajo, la tabla 3 Niveles de criticidad, explica loas significados

Cuadro 3. Niveles de criticidad

Impacto	Descripción
ALTO	El incidente de seguridad de la información puede afectar la continuidad del negocio de la Universidad Libre.
MEDIO	El incidente de seguridad de la información afecta a todo o a más de una dependencia de funcionarios de la Universidad Libre. (en este caso Seccionales a nivel nacional)
BAJO	El incidente afecta a un funcionario a un área de colaboradores de la Universidad Libre.
Fuente: autores	

Finalmente, la cuadro 4. Niveles de urgencia, muestra la combinación de las variables antes descritas.

Cuadro 4. Niveles de urgencia

Urgencia	Descripción
ALTO	El incidente de seguridad debe tener un tiempo de respuesta de (0-2 horas)
MEDIO	El incidente de seguridad debe tener un tiempo de respuesta de 2 a 4 horas
BAJO	El incidente de seguridad debe tener un tiempo de respuesta de 8 a 24 horas
Fuente: autores	

7.6. EQUIPOS DE RESPUESTA DE SEGURIDAD DE LA INFORMACIÓN (CSIRT)

Los equipos de respuesta a los Incidentes de Seguridad de la Información que no se consideren críticos estarán liderados por el Gestor de Incidentes de seguridad de la información de la Universidad Libre, y se conformaran por el dueño y el custodio de la información, de acuerdo con la matriz de levantamiento de activos de la Universidad Libre.

En caso de que el incidente de seguridad de la información se considere crítico, el Gestor de Incidentes de seguridad de la información de la Universidad Libre deberá proponer el equipo que considere deberá participar en el tratamiento del incidente, el cual será evaluado y aprobado por el CSIRT

Los equipos que se conformen podrán solicitar información o la participación de otros procesos, macro procesos u operadores estratégicos para la atención del incidente de seguridad de la información.

7.7 MITIGACIÓN DE DAÑOS Y DISMINUCIÓN DE RIESGOS

Es necesario proceder para minimizarlas consecuencias existentes de un incidente, de acuerdo a lo anterior puede ser el diferenciador entre que el impacto sea menor o de mayor importancia. La respuesta puntual obedecerá al origen del incidente al que se enfrente. No obstante, se sugieren las siguientes prioridades como punto de inicio:

• Resguardar la vida humana y la seguridad de las personas. Debe ser siempre la máxima prelación.

• Resguardar la información reservada y confidencial. Como parte del plan de respuesta a incidentes, se debe definir claramente qué información es Reservada o confidencial. Esto le permitirá constituir las prioridades para dar respuesta a la protección de datos.

• Resguardar otra información importante (por ejemplo, propiedad intelectual o del ámbito directivo). Hay otra información de su entorno de trabajo que también puede ser valiosa. Debe Resguardar en primer lugar los datos más valiosos antes de pasar a otros de baja prioridad.

• Resguardarla infraestructura física y tecnológica. Esto incluye Resguardarlos contra pérdida y/o modificación de los archivos de sistema y contra daños físicos al hardware. Los daños en los sistemas pueden tener como consecuencia un alto tiempo de inactividad.

• Reducir la perturbación de los recursos informático. Aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un incidente puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja.

En la actualidad hay distintas medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno, como mínimo, se debe llevar a cabo las siguientes acciones:

• Impedir que los posibles ciber delincuentes conozcan los procesos es que se adelanten dentro del tratamiento. De momento resulta difícil, porque algunas respuestas esenciales pueden alertar a los atacantes.

• Comparar el impacto de dejar sin conexión los sistemas en peligro y los sistemas relacionados, con el riesgo de continuar funcionando.

• Determinar los puntos de acceso usados por posibles atacantes, e implementar las medidas adecuadas para evitar futuros accesos.

• Considerar la opción de volver a crear un sistema con discos duros nuevos (se deben eliminar los discos duros existentes y almacenarlos, ya que se pueden usar como prueba si se decide procesar a los posibles atacantes). Asegurar el cambio de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.

7.8 PROCEDIMIENTO DE SEGUIMIENTO Y CIERRE

En esta etapa es cuando los reportes de eventos que fueron previamente valorados y clasificados como incidentes y que obtuvieron una respuesta, se procede a realizar el seguimiento oportuno, este seguimiento es realzado por la mesa de ayuda la cual es el canal principal donde fueron recibidas las solicitudes y se les fue creado un ticket de atención.

Durante el seguimiento se puede establecer si la respuesta al incidente es cerrarlo e impedir que no vuelva a ocurrir o mantenerlo y controlar su impacto de forma documental en el reporte de incidentes que relacione como fue contenido, que acciones fueron las ejecutadas para mitigar los daños, esta información se debe almacenar en la base de conocimiento que establezca las Universidad Libre como repositorio a la documentación generada.

Si durante el seguimiento se determina que el incidente detectado requiere un tratamiento urgente se deberá proceder con la mayor celeridad posible. Si la urgencia lo amerita, se deberá informar al jefe del área de sistemas. Para esta

información se debe tener en cuenta tipo de Incidente, nivel de criticidad, qué origino el incidente y como ocurrió.

Durante el seguimiento al incidente es posible que se necesite una asignación de un equipo con miras a atender el caso y poder dar una respuesta.

7.8.1 Asignar equipo. El equipo para el caso de la Universidad Libre corresponderá a las personas que conforman la dirección de sistemas debido a que son los encargados directos de dar respuesta a los incidentes.

En el caso que la Universidad Libre determine ampliar su planta y crear varios equipos de repuesta se tomaría como referencia los siguientes puntos para realizar un escalamiento de soporte más elevado que cumpla con un personal de :

- Mayor experiencia
- Recursos para solucionar temas más complejos o difíciles
- Mayor potestad para toma de decisiones.

Una vez clasificado y asignado el incidente el equipo registrara las acciones realizadas de forma procedimentalmente, siguiendo los siguientes pasos ejecutados en este orden:

- Evaluar la situación inicial
- Comunicar el incidente
- Contener el daño y minimizar el riesgo (se deben tener equipos pre configurados con las herramientas y programas necesarios para realizar el aislamiento del equipo en cuestión)
- Identificar el tipo y la gravedad del ataque
- Proteger las pruebas
- Notificar a los organismos externos si es necesario y pertinente.
- Recuperar los sistemas
- Compilar y organizar la documentación del incidente
- Valorar los daños y costos del incidente
- Revisar la documentación y actualizarla si es necesario.

7.9 RECOLECCIÓN DE EVIDENCIAS

Si dentro de la atención es necesario realizar una recolección de evidencia. Esta verificación es realizada por el oficial de seguridad y corresponde a que, si el incidente tuvo repercusiones graves acompañado de su criterio profesional, tomara decisión si ordena la recolección de evidencia o no.

Se debe tener en cuenta lo principios para la recolección de evidencia consignados en el RFC3227[22]

7.9.1 Capturar una imagen del sistema tan precisa como sea posible.

- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.

- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.

- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.

- Recoger la información según el orden de volatilidad (de mayor a menor).

- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

7.9.2 Orden de volatilidad. El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.

De acuerdo a esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.

[22] RIVAS LÓPEZ, Luís. Análisis Forense de sistemas informáticos. 2008. [en línea], [consultado el 23 de mayo de 2016]. Disponible en: lrivas.webs.uvigo.es/.../**Analisis**%20**forense**%20de%20 sistemas%20informaticos.pdf

- Disco
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

7.9.3 Acciones que deben evitarse. Se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en el caso de que sea necesario:

- No apagar el ordenador hasta que se haya recopilado toda la información.

- No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido como se explicará más adelante.

- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

7.9.4 Consideraciones sobre la privacidad

- Es muy importante tener en consideración las pautas de la Institución en lo que a privacidad se refiere. Es habitual solicitar una autorización por escrito de quien corresponda para poder llevar a cabo la recolección de evidencias. Este es un aspecto fundamental ya que puede darse el caso de que se trabaje con información confidencial o de vital importancia para la empresa, o que la disponibilidad de los servicios se vea afectada.

- No hay que entrometerse en la privacidad de las personas sin una justificación. No se deben recopilar datos de lugares a los que normalmente no hay razón para acceder, como ficheros personales, a menos que haya suficientes indicios.

7.9.4.1. Recolección. El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

7.9.4.2. Transparencia. Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes. Pasos a seguir para garantizar la trasparencia:

- ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.

- Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca.

- Fijar el orden de volatilidad para cada sistema.

- Obtener la información de acuerdo al orden establecido.

- Comprobar el grado de sincronización del reloj del sistema.

- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.

- Documentar cada paso.

- No olvidar a la gente involucrada. Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

7.9.4.3 Almacenamiento de evidencias. Cadena de custodia debe estar claramente documentada y se deben detallar los siguientes puntos:

- ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
- ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
- ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?
- En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de documento.

Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

7.9.4.4 Controlar incidente. De acuerdo a la causa detectada el control se aplicará; si se detecta que la falla fue de Software o Hardware se comunicara con el proveedor pertinente, si fue una vulnerabilidad detectada sede deberá actualizar para corregir la falla, si ocurre servicios de credenciales se deberán cambiar.

Si el incidente no es controlado se convoca un comité de seguridad donde participa el equipo o los líderes respectivos de acuerdo las directivas establecidas, con el fin de tomar una decisión frente al incidente que no se ha podido controlar.

El comité debe estar integrado por el oficial de seguridad el director de sistemas y el coordinador de sistemas del área de TI y sus funciones:

- Revisar y monitorear los incidentes de seguridad de la información
- Revisar y aprobar los proyectos de seguridad de la información
- Aprobar las modificaciones o nuevas políticas de seguridad de la información

Realizar otras actividades de alto nivel relacionadas con la seguridad de la información

Como resultado de comité se puede tomar la decisión de solicitar a un proveedor que asuma el control del incidente si es necesario un apoyo más especializado que se haga cargo.

7.10 PROCEDIMIENTO DE MEJORA CONTINUA

Una vez sean ejecutadas las actividades de atención y tratamiento del incidente, es necesario que se realice la fase procedimental de lecciones aprendidas las cuales se deberá retroalimentar sobre cómo fue atendido el incidente e identificar que se puede mejorar y/o cambiar para que en el futuro el modelo tenga la madurez suficiente. También se deben realizar actividades de:

Llevar a cabo el análisis forense de seguridad de la información, según se requiera.

- Identificar las lecciones aprendidas de los incidentes y vulnerabilidades de seguridad de la información.

- Revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información (controles nuevos y/o actualizados), al igual que la política de gestión de incidentes de seguridad de la información, como resultado de las lecciones aprendidas.

- Revisar, identificar, y si es posible, hacer mejoras a los resultados de la revisión por la dirección y la evaluación de riesgos para la seguridad de la información existentes, como resultado de las lecciones aprendidas.

- Revisar cómo fue la eficacia de los procesos, los procedimientos, los formatos de reporte y/o la estructura organizacional para responder a la evaluación y la recuperación de cada incidente de seguridad de la información y tratar las vulnerabilidades de seguridad de la información, y con base en las lecciones aprendidas identificar y hacer mejoras en el esquema de gestión de incidentes de seguridad de la información y su documentación.

- Actualizar la documentación.

- Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si la Universidad Libre lo desea).

8. PRUEBAS

Dentro del levantamiento, análisis de información que se llevó a cabo en la Universidad Libre referente a al diseño de un procedimiento de atención de incidentes de la seguridad de información se pudo establecer las siguientes pruebas siguiendo las recomendaciones propuestas:

8.1 CAPACITACIÓN DE INSTALACIÓN Y RESOLUCIÓN DE PROBLEMAS DEL ANTIVIRUS KASPERSKY

Se realizó la capacitación sobre la resolución de problemas más comunes presentados en el antivirus *Kaspersky* que corresponde a la herramienta que la Universidad Libre tiene instalada en sus equipos, esta capacitación fue dirigida al equipo de soporte técnico y a su coordinador. La figura 5 Asistencia capacitación, muestra evidencias del proceso de capacitación.

Figura 5. Lista Asistencia capacitación.

LISTA DE ASISTENCIA

FECHA: DD MM AAAA

TEMA: CAPACITACIÓN DE INSTALACIÓN Y RESOLUCIÓN DE PROBLEMAS DEL ANTIVIRUS KASPERSKY

DURACION: 1 HORA

RESPONSABLE: JOHN CHAVES

No.	NOMBRE PARTICIPANTE	CEDULA	CARGO	COREEO ELECTRÓNICO	FIRMA
1	Andrea Jiménez García	52'956286	Coordinadora	andrea.jimenez@unilibrebog	Andrea Jiménez
2	Karen Pamela Dorgelmo	1022393731321	Agente mesa de ayuda	Karen.Pamela@unilibre	Karen Pamela
3	Miguel Angel Caro R	1018422915	Técnico Soporte	miguel.caro@unilibrebog	
4	Guillermo Arregoces	1019033447	Tecnico Soporte	Guillermoarregoces@hotmail.com	
5	Juan Carlos Rodriguez	7707759096	tecnico soporte	Juan.Rodriguez@unili	
6	Jorge Luis Polo Ballen	1023007275	tecnico Soporte	Jorgeballen1@gmail.com	Jorge Polo
7	Cristian Castro	1024510166	Tecnico Soporte	cristian.castro@unilibrebog	
8					
9					
10					
11					
12					
13					
14					
15					

FIRMA DEL RESPONSABLE:

Fuente: autores

8.2 INFORME ANÁLISIS DE VULNERABILIDADES DE SERVIDORES DE LA UNIVERSIDAD LIBRE

Este informe efectúa una "evaluación de vulnerabilidad en línea" elaborada por la Universidad Libre. Este documento ha sido hecho y dispuesto para suministrar un informe rápido y fácil de entender para implicar la tarea de asegurar los sistemas informáticos y equipos informáticos conectados a Internet.

Las vulnerabilidades del sistema son clasificadas dentro de cuatro categorías: Riesgo Alto, Riesgo Medio, Riesgo Bajo, Información. De acuerdo con lo anterior se realiza un resumen ejecutivo que compila la información para una revisión a nivel de gerencia. Este resumen contiene tanto datos escritos como gráficos basados en el resultado del escaneo. Estos resultados incluyen información como "cuando se realizó el análisis", "que realizó el análisis" y la cantidad de vulnerabilidades del sistema que se encuentran en cada categoría.

Los detalles y los nombres de las vulnerabilidades descubiertas se encuentran en el capítulo Resumen de vulnerabilidades. Esto es seguido por las descripciones individuales para la corrección de cada punto vulnerable detectado. Cada vulnerabilidad descubierta en el sistema se suministra con una posible remediación.

8.2.1 Niveles de gravedad

8.2.1.1 Vulnerabilidades de Riesgo Alto. Cuando se identifica una vulnerabilidad de riesgo alto, significa que es posible que un intruso penetre y comprometa el sistema completamente y/o acceda a la información de alta sensibilidad del sistema. Esto a su vez podría conducir a la pérdida o robo de datos privados y sensibles.

8.2.1.2 Vulnerabilidades de Riesgo Medio. La identificación de una vulnerabilidad de riesgo medio, significa que un intruso puede obtener acceso a información del sistema que podría conducir a ataques más específicos y, posiblemente, a un compromiso de todo el sistema. Esto a su vez podría conducir a la pérdida o robo de datos privados y sensibles.

8.2.1.3 Vulnerabilidades de Riesgo Bajo. La identificación de una vulnerabilidad de riesgo bajo, por lo general significa que un intruso puede obtener acceso a la información del sistema que podría ayudar y dar lugar a ataques más específicos que resultan en la pérdida o robo de datos privados y sensibles.

8.2.1.4 Información. Todas las entradas de este nivel sólo tienen que proporcionar información adicional a la ya disponible sobre el sistema analizado. Esto no implica que el sistema sea o no vulnerable.

8.2.1.5 Resumen ejecutivo. Este informe es un análisis de seguridad realizado por la Universidad Libre. Contiene información confidencial sobre el estado de su red. El acceso a esta información por parte de personas no autorizadas puede permitir que pongan en peligro la seguridad de su red. Los detalles del objetivo evaluado se describen en la tabla 1 Dirección IP de prueba.

Este análisis se llevó a cabo por el usuario Admin.

Tabla 1. Dirección IP de prueba

Country	IP Addr	Started at	Ended at	Duration
0	10.1.10.27	2016.04.28 21.49	2016.04.28 21.49	00-00-00
Fuente: autores				

8.3 PERFIL DE ANÁLISIS

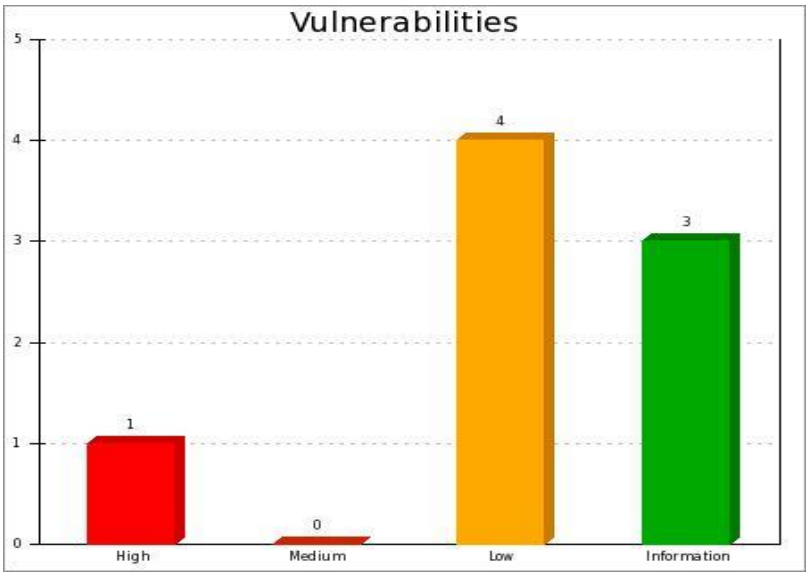
- Perfil de Análisis para IP 10.1.10.27: Normal Scan - 10.000 Most Common Ports *RECOMMENDED*

8.3.1 Nivel de seguridad general. Cat. 1 (*Critical Level*)

- Vulnerabilidades. Se identificaron Un total de 9, entre Vulnerabilidades potenciales e Información. Se han clasificado como sigue: 1 Alto, 0 Medio, 4 Bajo, 3 Información.

La grafica 1 muestra la representación de las vulnerabilidades encontradas.

Gráfica 1. Vulnerabilidades



Fuente: autores

- Traza. En la tabla 2,Tabla de la Traza se presenta el resultado de un traceroute desde la cuenta Admin para los sistemas de destino: traceroute to 10.1.10.27 (10.1.10.27), 15 hopsmáx., 60 bytepackets.

Tabla 2. Traza

Hop	Name	IP	Location	Avg (ms)	Graph
1	192.168.712			0.245	
2	10.2.1.1.			2.639	
3	10.2.6.31			3.830	
4	10.255.255.1	10.255.255.1		34.170	
5					
6	10.255.255.14	10.255.255.1		4.041	
7	10.1.10.27	10.1.10.27		8.190	
Fuente: autores					

- Puertos y Servicios Identificados. En la tabla 3 Puertos y Servicios identificados se presentan los puertos y servicios se han identificado en los sistemas examinados:

Ports y servicios para IP: 10.1.10.27

Tabla 3. Puertos y servicios

Port	Protocol	Status	Service
135	tcp	open	*DCE endpoint resolution*
139	tcp	open	*NETBIOS Session Service*
445	tcp	open	*Microsoft DS*
3389	tcp	open	*WS WBT Server*
8060	tcp	open	
8080	tcp	open	*HTTP Alternate (seeport 80)*
8081	tcp	open	*Sun Proxy Admin Service*
9000	tcp	open	*CS listener*
13000	tcp	open	
14000	tcp	open	*SCOTTY High Speed File transfer*
49152	tcp	open	
49153	tcp	open	
49154	tcp	open	
49155	tcp	open	
49156	tcp	open	
49157	tcp	open	
49189	tcp	open	
49190	tcp	open	
Fuente: autores			

- Versión Banner Identificado. El cuadro 5 *Banner* identificado muestra la Versión *Banner* de Servicio eran legibles en los sistemas examinados. Se

recomienda volver a configurar estos *banners* con información falsa o ninguna en absoluto.

Versión *Banners* para IP: 10.1.10.27

Cuadro 5. Banner identificado

Banner name	Http Versión Banner
Port	8080/tcp
Details	Apache/2.4.10 (Win 32) Open SSL/1.0.1. I mod.kscwc/2.4.
Solution	It is highly recommended to configure thist output to return boqus or notat ali it you have aiready done that please ignore this warning
Banner name	Http Versión Banner
Port	8081/tcp
Details	Apache/2.4.10 (Win 32) Open SSL/1.0.1. I mod.kscwc/2.4.
Solution	It is highly recommended to configure thist output to return boqus or notat ali it you have aiready done that please ignore this warning
Banner name	Http Versión Banner
Port	14000/tcp
Details	qSOAP/2.7.
Solution	It is highly recommended to configure thist output to return boqus or not at ali it you have aiready done that please ignore this warning
Fuente: autores	

Cuadro 5. Continuación

Banner name	Http Versión Banner
Port	8080/tcp
Details	Apache/2.4.10 (Win 32) Open SSL/1.0.1. I mod.kscwc/2.4.
Solution	It is highly recommended to configure thist output to return boqus or not at ali it you have aiready done that please ignore this warning
Fuente: autores	

8.4 RESUMEN DE VULNERABILIDADES

IP: 10.1.10.27

Vulnerabilidades Altas

- *OpenSSLmemoryCorruption*

Vulnerabilidades Bajas

- *It is possible to obtain remote NetBIOS name table.*

Informativas

- *AllProtocolsTested*

8.5. METODOLOGÍA DEL ANÁLISIS DE VULNERABILIDADES

La metodología que se usa para identificar las vulnerabilidades de los componentes o estructuras brindadas por el cliente, serán los ataques mediante el uso de la herramienta *Nessus.*

Una vez se han atacado se identificarán las vulnerabilidades en un rango de 4 etapas desde la más baja informativa, que comprende información con respecto a cosas básicas y buenas prácticas hasta la más alta a la cual se le hará una recomendación.

Como resultado se realizará un informe final en el cual se informarán todas las vulnerabilidades, con su respectivo detalle e información.

8.6 MEDIDAS DE MITIGACIÓN

La determinación de las medidas de mitigación, a partir de la estimación de la vulnerabilidad, permite programar más rápidamente acciones para reducir el efecto que tiene poseer esta vulnerabilidad en el sistema.

Estas medidas son el fruto de los análisis realizados y ejecutados sobre ellas, a continuación, se describen los elementos que intervienen a la hora de la mitigación.

Amenaza: Se deberá identificar la amenaza con la cual se trabajará.

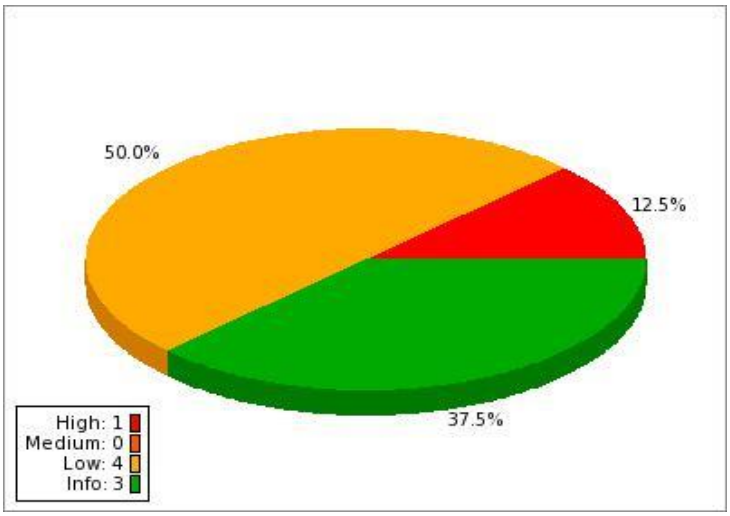
Estructuras físicas y equipos: Esto en el que caso de que se necesite actuar sobre un elemento físico como lo es un equipo o una estructura.

Organización empresarial y componentes de soporte y servicio: Este elemento de mitigación es no estructural, necesario a la hora de fortalecer las actividades operativas y técnicas, se debe saber cuándo es necesario un soporte por parte de un tercero para no caer en los riesgos de que se materialice la amenaza sobre la vulnerabilidad.

Operación y mantenimiento: Estas actividades son las más recomendadas ya que son o deberían ser parte de la vida cotidiana y tareas diarias, tales como el soporte, mantenimiento, actualización y parcheo de un sistema y de sus componentes.

La grafica 2 muestra el porcentaje de las vulnerabilidades encontradas en la IP: 10.1.10.27.

Gráfica 2. Vulnerabilidades de IP: 10.1.10.27



Fuente: autores

Vulnerabilidad I: Corrupción de memoria OpenSSL

- *OpenSSL*: Es un api que proporciona un entorno adecuado para encriptar los datos enviados a otra computadora dentro de una red y a su vez des encriptarlos adecuadamente por el receptor, evitando así, el acceso a la información por intrusos con la utilización de sniffer.

El conjunto de herramientas OpenSSL es una característica de FreeBSD que ofrece una capa cifrada de transporte sobre la capa normal de comunicación, permitiendo la combinación con muchas aplicaciones y servicios de red.

Impacto: El Open SSL identificado en esta versión es vulnerable a un ataque de corrupción de memoria. Esto puede permitir ataques remotos y exponer el sistema y hacer que los datos no sean de confianza. asn1_d2i_read_bio en OpenSSL contiene errores enteros al procesar datos de ASN.1. Este puede ser explotado con datos no confiables con certificados como X.509 o llaves públicas RSA. El servicio también está corriendo sobre el puerto 8081.

Solución: Actualizar a la última versión del software identificado.

9. CONCLUSIONES

Como resultado del presenta trabajo es posible concluir que la información y las tecnologías de la información, sugieren la necesidad de ser resguardadas bajo los principios de la seguridad informática: confidencialidad, integridad y disponibilidad.

Al aplicar estos principios a la información como activo importante en la Universidad Libre, nos sugiere la creación e implementación de un modelo de atención de incidentes informáticos, soportado en el diseño de procedimientos apropiados, con el fin de proteger y mitigar incidentes que se puedan presentar.

El conocimiento de la norma ISO/IEC 27035 y soportar los procedimientos diseñados sobre la norma, le permitirá a la dirección de sistemas de la Universidad Libre, abordar, contener y corregir las debilidades encontradas inicialmente y ofrecer una estructuración más alineada a los principios de la seguridad informática .

Tener establecidos unos criterios de criticidad que permitan evaluar el impacto del incidente de seguridad que pueda tener sobre la información, se hacen necesarios para establecer las medidas que se deberán aplicar para su mitigación y/o solución.

La experiencia realizando el presente trabajo nos demostró que la falta de concientizar a la comunidad educativa, docente y administrativa, es parte de los riesgos importantes que puede sufrir la información y que la preparación de la dirección de sistemas es vital para contrarrestar adecuadamente, el riesgo latente por las acciones que pueden generarse desde los diferentes actores que integran la Universidad Libre.

BIBLIOGRAFÍA

CENTRO DE COORDINACIÓN SEGURIDAD INFORMÁTICA COLOMBIA. ¿Qué es CSIRT? Equipo de respuestas ante emergencias informáticas. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: www.csirt-ccit.org.co

Diccionario de la lengua española. (s.f.). Diccionario de la lengua española | Edición del Tricentenario. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: http://dle.rae.es/?id=T8ktrp2

INFORMÁTICA FORENSE COLOMBIA. (s.f.). ¿Qué son los ordenadores cuánticos? ¿Qué aplicaciones tendrán? ¿Es la informática del futuro? [En línea], [consultado el 23 de mayo de 2016]. Disponible en: http://www. Informática forense.com.co/index.php/la-informática-forense

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Guía para la elaboración metodológica de un proyecto. Bogotá: ICONTEC.

ESSUS. (s.f.). Monitoreo continuo. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: *http://www.tenable.* com/products/nessus-vulnerability-scanner.

MINISTERIO DE LA TECNOLOGÍA, INDUSTRIA Y COMERCIO. Normas NTC-ISO-IEC 27035 - Tecnología de la información. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_Continuidad.pdf

RIVAS LÓPEZ, Luís. Análisis Forense de sistemas informáticos. 2008. [en línea], [consultado el 23 de mayo de 2016]. Disponible en: lrivas.webs.uvigo.es/.../ Análisis %20forense%20de%20 sistemas%20informaticos.pdf

UNIVERSIDAD DE CALIFORNIA. ¿Qué es FreeBSD? [En línea], [consultado el 23 de mayo de 2016]. Disponible en: https://es.wikipedia.org/wiki/FreeBSD

UNIVERSIDAD LIBRE DE COLOMBIA. Políticas de seguridad de la administración y protección de la Información en la Universidad Libre. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: www.unilibre.edu.co/...universitarias/153-nuestro-sistema-de-gestion-de-seguridad

_____. Seguridad de la información. [En línea], [consultado el 23 de mayo de 2016]. Disponible en: https://www.unilibre.gov.co/.../Portals/0/Documentos/